In the Claims:

This listing of claims will replace all prior versions and listings of claims in the application.

1-5. (canceled).

6. (currently amended) The method of claim [[1]] 76, wherein producing an array of session random encryption [[key]] keys at the first station includes:

providing a buffer at the first station;

generating said keys and storing said keys in the buffer;

associating respective session random key initiation intervals with said keys stored in said buffer;

[[using]] selecting keys from said buffer as said selected session random symmetric encryption key [[keys]] in response to corresponding requests received by said first station during said respective session random key initiation intervals ~~for use in a first exchange of said plurality of exchanges~~;

removing keys from said buffer after expiry of [[the]] respective session random key lifetimes, where the session random key lifetimes expire after the session random symmetric encryption key initiation intervals ~~lifetime in the buffer~~.

7. (original) The method of claim 6, wherein said buffer is managed as a circular buffer.

8. (original) The method of claim 6, wherein a session random key lifetime in the buffer for said plurality of exchanges has a value within which the plurality of exchanges can be completed in expected circumstances, and said keys are removed from said buffer after a multiple M times said value of session random key lifetime to engage into establishing a communication session, where M is less than or equal to 10.

9. (currently amended) The method of claim 6, wherein a session random key lifetime in the buffer for said plurality of exchanges has a value within which the plurality of exchanges can be completed in expected circumstances, and said keys are removed from said buffer after a

multiple M times said value, and the session random key lifetime to engage into establishing a communication session is less than about 90 ~~second~~ seconds.

10. (canceled).

11. (currently amended) The method of claim [[1]] 76, ~~wherein producing an encryption key at the first station includes:~~

~~assigning, in said first station, a session random key for use within a session random key initiation interval in response to requests received by said first station during said session random key initiation interval for use in a first exchange of said plurality of exchanges;~~

~~associating, in said first station, a plurality of intermediate data random keys with said request for use in said plurality of exchanges;~~

wherein said plurality of exchanges includes

a first exchange including sending a first message from the first station carrying said selected session random symmetric encryption key to the second station, where the second station returns a second message carrying ~~a shared parameter~~ the identifier of the second station encrypted using [[the]] said selected session random symmetric encryption key, and decrypting the ~~shared parameter~~ identifier of the second station at the first station to validate the second station, or a user at the second station; and

a second exchange including sending a further message from the first station to the second station, the further message carrying a particular data random symmetric encryption key from said sub-array ~~plurality of intermediate data random keys~~ encrypted using [[the]] said selected session random symmetric encryption key, where the second station returns another message carrying a hashed version of said particular data random symmetric key encrypted using said particular ~~encryption~~ data random symmetric key to the first station, and decrypting said hashed version of said particular data random symmetric key at the first station using said particular data random symmetric key.

12. (currently amended) The method of claim [[1]] 76, including ~~wherein producing an encryption key at the first station includes:~~

~~assigning, in said first station, a session random key for use within a session random key initiation interval in response to requests received by said first station during said session random key initiation interval for use in a first exchange of said plurality of exchanges;~~

~~associating, in said first station, a plurality of intermediate data random keys with said request for use in said plurality of exchanges; and~~

after said request for initiation of a communication session, presenting to the second station a user interface along with [[the]] said selected session random symmetric encryption key, said user interface including a prompt for entry of said identifier of the second station ~~a shared parameter~~ and at least one of said first and second shared secrets ~~secret~~.

13. (currently amended) The method of claim [[1]] 76, including ~~wherein producing an encryption key at the first station includes:~~

~~assigning, in said first station, a session random key for use within a session random key initiation interval in response to requests received by said first station during said session random key initiation interval for use in a first exchange of said plurality of exchanges;~~

~~associating, in said first station, a plurality of intermediate data random keys with said request for use in said plurality of exchanges; and~~

after said request for initiation of a communication session, presenting to the second station a user interface along with the session random key, said user interface including a prompt for entry of said identifier of the second station ~~a shared parameter~~ and said first and second ~~at least two~~ shared secrets.

14. (currently amended) The method of claim [[1]] 11, including ~~wherein producing an encryption key at the first station includes:~~

~~assigning, in said first station, a session random key for use within a session random key initiation interval in response to requests received by said first station during said session random key initiation interval for use in a first exchange of said plurality of exchanges;~~

~~associating, in said first station, a plurality of intermediate data random keys with said request for use in said plurality of exchanges;~~

~~wherein said plurality of exchanges includes~~

~~a first exchange including sending a first message from the first station carrying said session random key to the second station, where the second station returns a second message carrying a shared parameter encrypted using the session random key, and decrypting the shared parameter at the first station; and~~

~~a second exchange including sending a third message from the first station to the second station, the third message carrying a particular data random key from said plurality of intermediate data random keys encrypted using the session random key, where the second station returns a fourth message carrying a hashed version of said particular data random key encrypted using said particular data random key to the first station, and decrypting said hashed version of said particular data random key at the first station using said particular data random key;~~

~~and then~~ executing at least one additional exchange in said plurality of exchanges, where

said at least one additional exchange includes sending an additional message from the first station to the second station carrying a next data random symmetric key from said sub-array~~the plurality of intermediate data random keys associated with said request~~, encrypted using a data random symmetric key from said sub-array exchanged during a previously completed exchange in said plurality of exchanges, where the second station decrypts said next data random symmetric key and returns a responsive message carrying a hashed version of said next data random symmetric key encrypted using said next data random symmetric key, and decrypting at the first station said hashed version of said next data random symmetric key using said next data random symmetric key.

15. (canceled).

16. (original) The method of claim 14, including executing more than one of said additional exchanges.

17-21. (canceled).

22. (currently amended) The method of claim 76 [[17]], including upon request for initiation of a communication session, presenting to the second station a user interface for initiation of an authentication session including a compiled version of [[the]] said selected session random symmetric encryption key and parameters for one or more conversion arrays, said user interface including a prompt for entry of the said identifier of the second station ~~shared parameter~~ and at least one of said first and second shared secrets ~~secret~~.

23-24. (canceled).

25. (currently amended) The method of claim [[14]] 76, including ~~executing a further exchange including~~

~~sending a message from the first station to the second station carrying said encryption key encrypted using a first shared secret to the second station, where the second station returns a message carrying a hashed version of said encryption key encrypted using said first shared secret, and decrypting said encryption key at the first station;~~

~~sending a message from the first station to the second station carrying said encryption key encrypted using a second shared secret, where the second station decrypts said encryption key, and returns a message to the first station carrying a hashed version of the encryption key encrypted using said second shared secret; and~~

sending a message from the first station to the second station carrying an authentication signal indicating success or failure of mutual authentication and establishment of the final symmetric encryption key, said authentication signal being encrypted using one of said ~~intermediate~~ data random symmetric keys from a previous exchange in the plurality of exchanges.

26-30. (canceled).

31. (currently amended) The apparatus of claim [[26]] 77, wherein said logic to produce an array of session random symmetric encryption keys ~~provide ephemeral encryption~~ keys at the first station includes instructions:

providing a buffer at the first station;

generating said keys and storing said keys in the buffer;

associating respective session random key initiation intervals with said keys stored in said buffer;

[[using]] selecting keys from said buffer as said selected session random symmetric encryption keys in response to requests received by said first station during said respective session random key initiation intervals ~~for use in a first exchange of said plurality of exchanges~~;

removing keys from said buffer after expiry of the respective session random key lifetimes, where the session random key lifetimes expire after the session random key initiation intervals ~~lifetime in the buffer~~.

32. (original) The apparatus of claim 31, wherein said buffer is managed as a circular buffer.

33. (currently amended) The apparatus of claim 31, wherein a session random key lifetime in the buffer for said plurality of exchanges has a value within which the plurality of exchanges can be completed in expected circumstances, and said keys are removed from said buffer after a multiple M times said value ~~session random key lifetime~~ to engage into establishing a communication session, where M is less than or equal to 10.

34. (currently amended) The apparatus of claim 31, wherein a session random key lifetime in the buffer for said plurality of exchanges has a value within which the plurality of exchanges can be completed in expected circumstances, and said keys are removed from said buffer after a multiple M times said value ~~session random key lifetime~~ to engage into establishing a communication session, and the session random key lifetime to engage into establishing a communication session is less than about 90 seconds ~~second~~.

35. (canceled).

36. (currently amended) The apparatus of claim [[26]] 77, ~~wherein said logic to provide ephemeral encryption keys at the first station includes instructions:~~

~~assigning, in said first station, a session random key for use within a session random key initiation interval in response to requests received by said first station during said session random key initiation interval for use in a first exchange of said plurality of exchanges;~~

~~associating, in said first station, a plurality of intermediate data random keys with said request for use in said plurality of exchanges;~~

wherein said plurality of exchanges includes

a first exchange including sending a first message from the first station carrying said selected session random symmetric encryption key to the second station, where the second station returns a second message carrying said identifier of the second station ~~a shared parameter~~ encrypted using [[the]] said selected session random symmetric encryption key, and decrypting said identifier of the second station ~~the shared parameter~~ at the first station to validate the second station; and

a second exchange including sending a further message from the first station to the second station, the further message carrying a particular data random symmetric key from said sub-array ~~plurality of intermediate data random keys~~ encrypted using [[the]] said selected session random key, where the second station returns another message carrying a hashed version of said particular data random symmetric key encrypted using said particular ~~encryption~~ data random symmetric key to the first station, and decrypting said hashed version of said particular data random symmetric key at the first station using said particular data random symmetric key.

37. (currently amended) The apparatus of claim [[26]] 77, ~~wherein said logic to provide ephemeral encryption keys at the first station includes instructions:~~

~~assigning, in said first station, a session random key for use within a session random key initiation interval in response to requests received by said first station during said session random key initiation interval for use in a first exchange of said plurality of exchanges;~~

~~associating, in said first station, a plurality of intermediate data random keys with said request for use in said plurality of exchanges; and~~

logic to present, after said request for initiation of a communication session, ~~presenting~~ to the second station a user interface along with the selected session random symmetric encryption key, said user interface including a prompt for entry of said identifier of the second station ~~a shared parameter~~ and at least one of said first and second shared secrets ~~secret~~.

38. (currently amended) The apparatus of claim [[26]] 77, ~~wherein said logic to provide ephemeral encryption keys at the first station includes instructions:~~

~~assigning, in said first station, a session random key for use within a session random key initiation interval in response to requests received by said first station during said session random key initiation interval for use in a first exchange of said plurality of exchanges;~~

~~associating, in said first station, a plurality of intermediate data random keys with said request for use in said plurality of exchanges; and~~

logic to present, after said request for initiation of a communication session, ~~presenting~~ to the second station a user interface along with the selected session random symmetric encryption key, said user interface including a prompt for entry of said identifier of the second station ~~a shared parameter~~ and ~~at least two~~ said first and second shared secrets.

39. (currently amended) The apparatus of claim [[26]] 36, ~~wherein said logic to provide ephemeral encryption keys at the first station includes instructions:~~

~~assigning, in said first station, a session random key for use within a session random key initiation interval in response to requests received by said first station during said session random key initiation interval for use in a first exchange of said plurality of exchanges;~~

~~associating, in said first station, a plurality of intermediate data random keys with said request for use in said plurality of exchanges;~~

wherein said plurality of exchanges includes

~~a first exchange including sending a first message from the first station carrying said session random key to the second station, where the second station returns a second message carrying a shared parameter encrypted using the session random key, and decrypting the shared parameter at the first station; and~~

~~a second exchange including sending a third message from the first station to the second station, the third message carrying a particular data random key from said plurality of intermediate data random keys encrypted using the session random key, where the second station returns a fourth message carrying a hashed version~~

~~of said particular data random key encrypted using said particular data random key to the first station, and decrypting said hashed version of said particular data random key at the first station using said particular data random key;~~

~~and then executing~~ at least one additional exchange in said plurality of exchanges, where

said at least one additional exchange includes sending an additional message from the first station to the second station carrying a next data random symmetric key from said sub-array~~the plurality of intermediate data random keys associated with said request~~, encrypted using a data random symmetric key from said sub-array exchanged during a previously completed exchange in said plurality of exchanges, where the second station decrypts said next data random symmetric key and returns a responsive message carrying a hashed version of said next data random symmetric key encrypted using said next data random symmetric key, and decrypting at the first station said hashed version of said next data random symmetric key using said next data random symmetric key.

40. (canceled).

41. (original) The apparatus of claim 39, including logic executing more than one of said additional exchanges.

42-46. (canceled).

47. (currently amended) The apparatus of claim 77 [[42]], including upon request for initiation of a communication session, logic to present to the second station a user interface for initiation of an authentication session including a compiled version of the session random symmetric encryption key and parameters for one or more conversion arrays, said user interface including a prompt for entry of said identifier of the second station ~~the shared parameter~~, and at least one of said first and second shared secrets ~~secret~~.

48-49. (canceled).

50. (currently amended) The apparatus of claim [[39]] 77, including logic executing a further exchange including instructions

~~sending a message from the first station to the second station carrying said encryption key encrypted using a first shared secret to the second station, where the second station returns a message carrying a hashed version of said encryption key encrypted using said first shared secret, and decrypting said encryption key at the first station;~~

~~sending a message from the first station to the second station carrying said encryption key encrypted using a second shared secret, where the second station decrypts said encryption key, and returns a message to the first station carrying a hashed version of the encryption key encrypted using said second shared secret; and~~

sending a message from the first station to the second station carrying an authentication signal indicating success or failure of mutual authentication and establishment of the final symmetric encryption key, said authentication signal being encrypted using one of said ~~intermediate~~ data random symmetric keys from a previous exchange in the plurality of exchanges.

51-55. (canceled).

56. (currently amended) The article of claim 78 [[51]], wherein said logic to produce an array of session random symmetric encryption keys ~~provide ephemeral encryption~~ keys at the first station includes instructions:

providing a buffer at the first station;

generating said keys and storing said keys in the buffer;

associating respective session random key initiation intervals with said keys stored in said buffer;

[[using]] selecting keys from said buffer as said selected session random symmetric encryption keys in response to requests received by said first station during said respective session random key initiation intervals ~~for use in a first exchange of said plurality of exchanges~~;

removing keys from said buffer after expiry of the respective session random key lifetimes, where the session random key lifetimes expire after the session random key initiation intervals ~~lifetime in the buffer~~.

57. (original) The article of claim 56, wherein said buffer is managed as a circular buffer.

58. (currently amended) The article of claim 56, wherein a session random key lifetime in the buffer for said plurality of exchanges has a value within which the plurality of exchanges can be completed in expected circumstances, and said keys are removed from said buffer after a multiple M times said value ~~of session random key lifetime~~ to engage into establishing a communication session, where M is less than or equal to 10.

59. (original) The article of claim 56, wherein a session random key lifetime in the buffer for said plurality of exchanges has a value within which the plurality of exchanges can be completed in expected circumstances, and said keys are removed from said buffer after a multiple M times said value, and the session random key lifetime to engage into establishing a communication session is less than about 90 seconds.

60. (canceled).

61. (currently amended) The article of claim 78 [[51]], ~~wherein said logic to provide ephemeral encryption keys at the first station includes instructions:~~

~~assigning, in said first station, a session random key for use within a session random key initiation interval in response to requests received by said first station during said session random key initiation interval for use in a first exchange of said plurality of exchanges;~~

~~associating, in said first station, a plurality of intermediate data random keys with said request for use in said plurality of exchanges;~~

wherein said plurality of exchanges includes

a first exchange including sending a first message from the first station carrying said selected session random symmetric encryption key to the second station, where the second station returns a second message carrying said identifier of the second station ~~a shared parameter~~ encrypted using [[the]] said selected session random symmetric encryption key, and decrypting said identifier of the second station ~~the shared parameter~~ at the first station to validate the second station; and

a second exchange including sending a further message from the first station to the second station, the further message carrying a particular data random symmetric key from said sub-array ~~plurality of intermediate data random keys~~ encrypted using [[the]] said selected session random key, where the second station returns another message carrying a hashed version of said particular data random symmetric key encrypted using said particular ~~encryption~~ data random symmetric key to the first station, and decrypting said hashed version of said particular data random symmetric key at the first station using said particular data random symmetric key.

62. (currently amended) The article of claim 78 [[51]], ~~wherein said logic to provide ephemeral encryption keys at the first station includes instructions:~~

~~assigning, in said first station, a session random key for use within a session random key initiation interval in response to requests received by said first station during said session random key initiation interval for use in a first exchange of said plurality of exchanges;~~

~~associating, in said first station, a plurality of intermediate data random keys with said request for use in said plurality of exchanges; and~~

logic to present, after said request for initiation of a communication session, ~~presenting~~ to the second station a user interface along with the selected session random symmetric encryption key, said user interface including a prompt for entry of said identifier of the second station ~~a shared parameter~~ and at least one of said first and second shared secrets ~~secret~~.

63. (currently amended) The article of claim 78 [[51]], ~~wherein said logic to provide ephemeral encryption keys at the first station includes instructions:~~

~~assigning, in said first station, a session random key for use within a session random key initiation interval in response to requests received by said first station during said session random key initiation interval for use in a first exchange of said plurality of exchanges;~~

~~associating, in said first station, a plurality of intermediate data random keys with said request for use in said plurality of exchanges; and~~

logic to present, after said request for initiation of a communication session, ~~presenting~~ to the second station a user interface along with the selected session random symmetric encryption key, said user interface including a prompt for entry of said identifier of the second station ~~a shared parameter~~ and ~~at least two~~ said first and second shared secrets.

64. (currently amended) The article of claim 61 [[51]], ~~wherein said logic to provide ephemeral encryption keys at the first station includes instructions:~~

~~assigning, in said first station, a session random key for use within a session random key initiation interval in response to requests received by said first station during said session random key initiation interval for use in a first exchange of said plurality of exchanges;~~

~~associating, in said first station, a plurality of intermediate data random keys with said request for use in said plurality of exchanges;~~

wherein said plurality of exchanges includes

~~a first exchange including sending a first message from the first station carrying said session random key to the second station, where the second station returns a second message carrying a shared parameter encrypted using the session random key, and decrypting the shared parameter at the first station; and~~

~~a second exchange including sending a third message from the first station to the second station, the third message carrying a particular data random key from said plurality of intermediate data random keys encrypted using the session random key, where the second station returns a fourth message carrying a hashed version of said particular data random key encrypted using said particular data random key to the first station, and decrypting said hashed version of said particular data random key at the first station using said particular data random key;~~

~~and then executing~~ at least one additional exchange in said plurality of exchanges, where

said at least one additional exchange includes sending an additional message from the first station to the second station carrying a next data random symmetric key from said sub-array~~the plurality of intermediate data random keys associated with said~~

~~request~~, encrypted using a data random symmetric key from said sub-array exchanged during a previously completed exchange in said plurality of exchanges, where the second station decrypts said next data random symmetric key and returns a responsive message carrying a hashed version of said next data random symmetric key encrypted using said next data random symmetric key, and decrypting at the first station said hashed version of said next data random symmetric key using said next data random symmetric key.

65. (canceled).

66. (original) The article of claim 64, including logic executing more than one of said additional exchanges.

67-71. (canceled).

72. (currently amended) The article of claim 78 [[67]], including upon request for initiation of a communication session, logic to present to the second station a user interface for initiation of an authentication session including a compiled version of the session random symmetric encryption key and parameters for one or more conversion arrays, said user interface including a prompt for entry of said identifier of the second station ~~the shared parameter~~, and at least one of said first and second shared secrets ~~secret~~.

73-74. (canceled).

75. (currently amended) The article of claim 78 [[64]], including logic executing a further exchange including instructions

~~sending a message from the first station to the second station carrying said encryption key encrypted using a first shared secret to the second station, where the second station returns a message carrying a hashed version of said encryption key encrypted using said first shared secret, and decrypting said encryption key at the first station;~~

~~sending a message from the first station to the second station carrying said encryption key encrypted using a second shared secret, where the second station decrypts said encryption key, and returns a message to the first station carrying a hashed version of the encryption key encrypted using said second shared secret; and~~

sending a message from the first station to the second station carrying an authentication signal indicating success or failure of mutual authentication and establishment of the final symmetric encryption key, said authentication signal being encrypted using one of said ~~intermediate~~ data random symmetric keys from a previous exchange in the plurality of exchanges.

76. (new) A method for creating and securely distributing ephemeral random symmetric keys for use in a plurality of concurrent or spaced in time communication sessions on a communication medium between a first data processing station and a plurality of second data processing stations having access to the communication medium, in which the first station and each second station in the plurality of second stations have respective identifiers and first and second shared secrets, and for mutual authentication of the first and second stations without exchanging messages carrying said shared secrets via the communication medium, comprising:

receiving at the first station requests from the plurality of second stations for initiation of a communication session;

producing an array of session random symmetric encryption keys and plurality of sub-arrays of data random symmetric keys at the first station, where each sub-array is subordinated only to a respective session random symmetric encryption key to service a plurality of communication sessions by continuously generating, storing and obliterating the keys in the array and in the sub-arrays according to a logic at the first station; and

after receiving a request from a particular second station, selecting a session random symmetric encryption key from said array, and executing a plurality of exchanges of encrypted messages across said communication medium during an authentication stage of the communication session, the exchanges in the plurality of exchanges including at least one message carrying respective data random symmetric keys from the sub-array which is subordinated to the selected session random symmetric encryption key from the first station to the second station and messages respectively returning the data random symmetric keys, or their hashed equivalents, in an encrypted form from the second station to the first station, to mutually authenticate the first station and the second station without exchanging the first and second shared secrets over the communication medium, and to provide one of the data random symmetric keys from the sub-array to the second station as a final symmetric encryption key for use in subsequent communications during said communication session;

wherein in at least one of the plurality of exchanges, the respective data random symmetric key, or its hashed equivalent, is encrypted using an intermediate data random symmetric encryption key, where the intermediate data random symmetric encryption key is one of the data random symmetric keys from said sub-array, exchanged in a previous one of the plurality of exchanges; and

wherein in at least one of the plurality of exchanges, the respective data random symmetric key, or its hashed equivalent, is veiled in a conversion array using the first shared secret and then, encrypted using one of the data random symmetric keys from said sub-array exchanged in a previous exchange, and

in at least one other of the plurality of exchanges, the respective data random symmetric key, or its hashed equivalent, is veiled in a conversion array using the second shared secret and then, encrypted using one of the data random symmetric keys from said sub-array exchanged in a previous exchange.

77. (new) A data processing apparatus for creating and securely distributing ephemeral random symmetric keys for use in a plurality of concurrent or spaced in time communication sessions on a communication medium between the data processing apparatus as a first station and a plurality of second data processing stations having access to the communication medium, in which the first station and each second station in the plurality of second stations have respective identifiers and first and second shared secrets, and for mutual authentication of the first and second stations without exchanging messages carrying said shared secrets via the communication medium, comprising:

a processor at the first station, a communication interface adapted for connection to a communication medium, and memory storing instructions for execution by the data processor, the instructions including

logic to receive requests via the communication interface from the plurality of second stations for initiation of a communication session;

logic to produce an array of session random symmetric encryption keys and plurality of sub-arrays of data random symmetric keys at the first station, where each sub-array is subordinated only to a respective session random symmetric encryption key to service a plurality of communication sessions by continuously generating, storing and obliterating the keys in the array and in the sub-arrays; and

logic to select, after receiving a request from a particular second station, a session random symmetric encryption key from said array, and to execute a plurality of exchanges of encrypted messages across said communication medium during an authentication stage of the communication session, the exchanges in the plurality of exchanges including at least one message carrying respective data random symmetric keys from the sub-array which is subordinated to the selected session random symmetric encryption key from the first station to the second station and messages respectively returning the data random symmetric keys, or their hashed equivalents, in an encrypted form from the second station to the first station, to mutually authenticate the first station and the second station without exchanging the first and second shared secrets over the communication medium, and to provide one of the data random symmetric keys from the sub-array to the second station as a final symmetric encryption key for use in subsequent communications during said communication session;

wherein in at least one of the plurality of exchanges, the respective data random symmetric key, or its hashed equivalent, is encrypted using an intermediate data random symmetric encryption key, where the intermediate data random symmetric encryption key is one of the data random symmetric keys from said sub-array, exchanged in a previous one of the plurality of exchanges; and

wherein in at least one of the plurality of exchanges, the respective data random symmetric key, or its hashed equivalent, is veiled in a conversion array using the first shared secret and then, encrypted using one of the data random symmetric keys from said sub-array exchanged in a previous exchange, and

in at least one other of the plurality of exchanges, the respective data random symmetric key, or its hashed equivalent, is veiled in a conversion array using the second shared secret and then, encrypted using one of the data random symmetric keys from said sub-array exchanged in a previous exchange.

78. (new) An article of manufacture, comprising:

a machine readable data storage medium having computer program instructions stored therein, for creating and securely distributing ephemeral random symmetric keys for use in a plurality of concurrent or spaced in time communication sessions on a communication medium between a first data processing station and a plurality of second data processing stations having access to the communication medium, in which the first station and each second station in the plurality of second stations have respective identifiers and first and second shared secrets, and for mutual authentication of the first and second stations without exchanging messages carrying said shared secrets via the communication medium, said instructions comprising:

logic to receive at the first station requests from the plurality of second stations for initiation of a communication session;

logic to produce an array of session random symmetric encryption keys and plurality of sub-arrays of data random symmetric keys at the first station, where each sub-array is subordinated only to a respective session random symmetric encryption key to service a plurality of communication sessions by continuously generating, storing and obliterating the keys in the array and in the sub-arrays; and

logic to select, after receiving a request from a particular second station, a session random symmetric encryption key from said array, and to execute a plurality of exchanges of encrypted messages across said communication medium during an authentication stage of the communication session, the exchanges in the plurality of exchanges including at least one message carrying respective data random symmetric keys from the sub-array which is subordinated to the selected session random symmetric encryption key from the first station to the second station and messages respectively returning the data random symmetric keys, or their hashed equivalents, in an encrypted form from the second station to the first station, to mutually authenticate the first station and the second station without exchanging the first and second shared secrets over the communication medium, and to provide one of the data random symmetric keys from the sub-array to the second station as a final symmetric encryption key for use in subsequent communications during said communication session;

wherein in at least one of the plurality of exchanges, the respective data random symmetric key, or its hashed equivalent, is encrypted using an intermediate data random symmetric encryption key, where the intermediate data random symmetric encryption key is one of the data random symmetric keys from said sub-array, exchanged in a previous one of the plurality of exchanges; and

wherein in at least one of the plurality of exchanges, the respective data random symmetric key, or its hashed equivalent, is veiled in a conversion array using the first shared secret and then, encrypted using one of the data random symmetric keys from said sub-array exchanged in a previous exchange, and

in at least one other of the plurality of exchanges, the respective data random symmetric key, or its hashed equivalent, is veiled in a conversion array using the second shared secret and then, encrypted using one of the data random symmetric keys from said sub-array exchanged in a previous exchange.

///